УДК 004.056.053

***Н.А. Маслова***
Донецкий национальный технический университет, г. Донецк, Украина
masgpp@list.ru

# Методы оценки эффективности систем защиты информационных систем

В работе классифицирован подход к определению качества систем защиты информации, приведены показатели оценки качества и особенности расчета показателей. Описана модификация алгоритма Балаша, позволяющая минимизировать вычислительные затраты за счет использования целочисленных переменных, операций сложения и вычитания и выбора лучшего направления спуска по дереву решений, присущего методам типа ветвей и границ. Предложена методика оценки вычислительной сложности алгоритма, использующего эту модификацию.

## Введение

Высокие требования, предъявляемые к уровню информационной безопасности компаний, использование систем связи и передачи данных предопределяют необходимость проведения оценки эффективности систем защиты. Это сложная организационно-технологическая задача, решение которой находится комплексно и требует системного подхода.

Трудности определения количественных и качественных оценок эффективности системы защиты информации (СЗИ), а следовательно, и объективного подтверждения эффективности СЗИ, коренятся в несовершенстве существующего нормативно-методического обеспечения информационной безопасности в сложившихся в информационных технологиях подходах, которые принципиально отличаются от разработанных в традиционной инженерии. Недостаточно проработана система показателей информационной безопасности, в неудовлетворительном состоянии находятся критерии безопасности.

Как отмечали участники конференции директоров по информационной безопасности Russian CSO Summit-2008, академических работ по этой теме проводится очень мало, а постоянно изменяющийся перечень угроз и отсутствие единого подхода к оценке эффективности СЗИ делает поставленную задачу необходимой и актуальной.

## Анализ исследований и предшествующие публикации

Существует обширная литература, посвященная проблемам информационной безопасности в информационных системах и сетях передачи и обработки информации. Задачи создания, организации и исследования процессов функционирования, совершенствования и развития СЗИ в той или иной степени нашли отражение в трудах ряда отечественных и зарубежных ученых, среди которых Е.С. Вентцель, В.Ю. Гайкович, В.А. Галатенко, В.А. Герасименко, В.И. Гарбарчук, Ю.В. Демченко, В.И. Завгородний, В.К. Задирака, А.Г. Карпов, В.В. Лебедев, В.В. Мельников, В.С. Михалевич, А.Н. Назаров, А.С. Олексюк, А.Ю. Першин, А.З. Пескозуб, А.П. Пятибратов, В.К. Размахнин, С.П. Расторгуев, Ю. Самохин, И.В. Сергиенко, А.В. Соколов, А.В. Спе-

сивцев, С.Е. Сталенков, Г.В. Фоменков, Ю.В. Щеглов, С. Шатт, Д. Шепелявый, Г.Е. Шепитько, В.В. Шураков, В.Ф. Шаньгин и многие другие [1-4]. Исследования ряда проблем в указанной области проводились и автором статьи [5]. Однако до настоящего времени в полной мере не изучены и остаются дискуссионными методологические, методические и практические аспекты исследования целевой и экономической эффективности сложных систем.

## Цель работы

Целью выполнения работы явились: анализ и систематизация методов оценки систем защиты информации, разработка концептуальной методики оценки эффективности системы защиты информации с использованием модификаций современных алгоритмов.

## Основной материал

Информационная система – это сложная, распределенная в пространстве система, состоящая из множества сосредоточенных (локальных) подсистем (информационных узлов), располагающих программно-аппаратными средствами реализации информационных технологий, и множества средств, обеспечивающих соединение и взаимодействие этих подсистем с целью предоставления территориально удаленным пользователям широкого набора услуг из сферы информационного обслуживания.

Наличие средств защиты информации является характерной чертой любой современной информационной системы. Эффективность защиты информации в информационных системах достигается применением средств защиты информации.

В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

– обеспечивающие разграничение доступа к информации в автоматизированных системах;
– обеспечивающие защиту информации при передаче ее по каналам связи;
– обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
– обеспечивающие защиту от воздействия программ-вирусов;
– обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Однако ни одно отдельно выбранное средство защиты информации не может защитить от многообразия существующих угроз безопасности, а простая комбинация разнообразных средств защиты приводит к снижению эффективности защиты в целом из-за возможной конфликтности разрозненных средств защиты. Поэтому в последнее время наметилась тенденция к построению сложных систем информационной безопасности.

Система защиты информации (СЗИ) – это сложный комплекс программных, технических, криптографических организационных и иных средств, методов и мероприятий, предназначенных для защиты информации.

Эффективность СЗИ можно охарактеризовать как способность системы противостоять несанкционированным действиям нарушителя в рамках проектной угрозы. Таким образом, эффективность СЗИ и характеризует уровень защищенности объекта. Существуют качественные и количественные методы анализа эффективности СЗИ. Во многих

случаях качественных оценок не достаточно, чтобы ответить на вопрос, насколько надежна защита объекта. Более точны количественные методы. Однако для того, чтобы «измерить» эффективность, необходимо иметь обоснованный критерий (показатель оценки эффективности системы). На практике встречаются следующие типы критериев.

1. Критерии типа «эффект-затраты», позволяющие оценивать достижение целей функционирования СЗИ при заданных затратах (так называемая экономическая эффективность).

2. Критерии, позволяющие оценить качество СЗИ по заданным показателям и исключить те варианты, которые не удовлетворяют заданным ограничениям. При этом используются методы многокритериальной оптимизации, восстановления функций и функционалов, методы дискретного программирования.

3. Искусственно сконструированные критерии, позволяющие оценивать интегральный эффект (например, «линейная свертка» частных показателей, методы теории нечетких множеств).

Для оценки качества системы защиты могут быть использованы международные стандарты ISO/IEC 17799 и ISO/IEC 15408. В первом из них предлагается расширенный перечень аспектов информационной безопасности. Он начинается с принципов разработки политики безопасности, включает основы проверки системы на соответствие требованиям информационной безопасности, содержит практические рекомендации.

Стандарт ISO/IEC 15408 определяет критерии безопасности информационных технологий. В нем не приводится список требований по безопасности, но положения стандарта позволяют сформулировать цели безопасности, направленные на обеспечение противостояния угрозам и выполнение политики безопасности, т.е. те цели, которые должны использоваться как основа для оценки свойств безопасности продуктов, систем и информационных технологий. Стандарт описывает инфраструктуру, в которой пользователи системы могут сформулировать требования, а эксперты по безопасности определить, обладает ли продукт заявленными свойствами.

Эффективность функционирования СЗИ зависит от множества действующих взаимосвязанных между собой элементов и, как правило, оценивается совокупностью критериев, находящихся в сложных конфликтных взаимоотношениях.

Отсутствие на сегодняшний день общего подхода к решению задач данного класса закономерно влечет за собой многообразие различных не взаимосвязанных методов оценки качества.

Процесс определения эффективности систем защиты начинают с выбора и обоснования показателей (критериев) оценки эффективности системы защиты, а затем переходят к подбору или разработке методик расчета этих показателей. В табл. 1 приведены условные названия используемого подхода к выбору критериев и оценке параметров, показатели эффективности систем защиты и методики их расчета.

Наиболее распространенными методами оценки эффективности СЗИ, используемыми при так называемом оптимизационном или комбинаторном подходе, являются: аддитивный метод Балаша и метод ветвей и границ, относящийся к классу задач дискретного программирования с булевыми переменными. Указанные методы используются как для построения новой СЗИ, так и для оценки качественных характеристик существующей СЗИ или выбора оптимальной СЗИ из набора, рекомендуемого к применению.

Таблица 1 – Показатели оценки эффективности систем защиты и методики их расчета

| | Подход к оценке СЗИ | Показатели оценки эффективности | Способ расчета показателей |
|---|---|---|---|
| 1. | Статистичес-кий. | Угроза i-го типа возникает в среднем за период времени Ti. | Статистическая обработка потенциальных угроз и их последствий. |
| 2. | Вероятностный. | Суммарные средние потери $R = \sum_{i=1}^{2^n} \sum_{j=1}^{2^n} P(\vec{\gamma} / \vec{s}) P(\vec{s}) \Pi(\vec{\gamma}, \vec{s}) + m,$ $P(\vec{\gamma} / \vec{s})$ – вероятность устранения; $P(\vec{s})$ – априорная вероятность состояния объекта контроля, $\Pi(\vec{\gamma}, \vec{s})$ – потери принятия решения s при состоянии объекта s, m – количество распознаваемых угроз. | Определяется вероятность отказа системы от обработки данных в результате реализации угроз. |
| 3. | Частотный. | Ожидаемый ущерб от i-й угрозы: $R_i = F(S,V)$, где S – показатель частоты возникновения угрозы; V – условный показатель ущерба. | На основании анализа статистического материала задается значение S, величина V выбирается равной от 1 до max возможной суммы ущерба, рассчитывается значение показателя $R_i$ как функции параметров V и S. |
| 4. | Экспертное оценивание. | Степень обеспечения безопасности SR системы S $SR_{(s,r)} = \frac{1}{n_{i-1}^{n}} W_i G_i,$ | Определяется количество (n) и перечень пара-метров, (i) характеризующих СЗИ. Задаются значе-ния субъективных коэффициентов важности ($W_i$) каждой из характеристик $G_i$, назначенные эксперт-ным путем. Рассчитывается значение параметра SR. |

Продолж. табл. 1

| | | | |
|---|---|---|---|
| 5. | Информационно-энтропийный. | Величина информационной энтропии Шеннона: $\psi(t) = (\int_0^t s_n(t-\tau)...(\int_0^t s_3(\int_0^t s_1(\tau)s_2(t-\tau)d\tau)d\tau...)d\tau$ $s_1, \dots s_n$ – значения информационных энтропий различных подсистем. | Проводится аналитическое вычисление информационной энтропии системы, используя понятие свертки функций. При линейной зависимости эффективность интеграции подсистем в информационном плане считают удовлетворительной. В противном случае – неэффективной [6]. |
| 6. | Нейросетевой подход (многокритериальная оценка). | Нечёткие показатели защиты информационной системы в виде лингвистических переменных, таких как: «абсолютно незащищённая», «недостаточно защищённая», «защищённая», «достаточно защищённая», «абсолютно защищённая» $A = \sum_{i=1}^{n} \frac{\mu^A(x_i)}{x_i}$. | Принадлежность определённого уровня безопасности определяется на промежутке [0, 1], показатели надёжности являются функцией принадлежности $\mu^A(x_i)$, где $x_i$ – есть элемент множества X – требований безопасности, A – множество значений, определяющих выполнение требований безопасности. Оценка эффективности производится по чётко определённым критериям [7]. |
| 7. | Метод минимизации рисков. | Показатель экономического эффекта от управления рисками рассчитаем по формуле, учитывающей $M_0$ - суммарные вероятные потери без обработки идентифицированных рисков; суммарные вероятные потери после обработки рисков M; суммарные фактические потери от проявления рисков $I_Ф$; суммарные фактические расходы на обработку идентифицированных рисков ($H = H_Ф$); суммарные фактические потери от проявления рисков $I_{Фн}$; суммарные фактические расходы на обработку рисков $H_{Фн}$) | 1. Произвести фиксацию рисков.<br>2. Определить индекс риска (может быть выражен относительным или абсолютным уровнем затрат и измеряется вероятностью возникновения риска и степенью влияния риска при его возникновении).<br>3. Классификация рисков по степени воздействия и по уровню влияния.<br>4. Определение способов обработки риска.<br>5. Расчет показателей, характеризующих риски.<br>6. Расчет показателя экономического эффекта от управления рисками. |

Продолж. табл. 1

| | | | |
|---|---|---|---|
| | | $E=(\sum_{i=1}^{N}M_{oi}-\sum_{i=1}^{N}M_i)-((\sum_{i=1}^{N}I_{\phi i}+\sum_{i=1}^{N}H_{\phi i})+(\sum_{j=1}^{K}I_{\phi нj}+\sum_{j=1}^{K}H_{\phi нj}))$. | |
| 8. | Матричный (формальные модели защиты) | Состояние системы защиты описывается тройкой параметров, например:<br>(S,O,M) – множества S – субъектов, O – объектов, M – прав доступа;<br>Или (O,H,M) – O – основы и составные части системы (нормативно-правовая, организационная, информационная и т.д.)<br>H – направления защиты, M – этапы создания СЗИ. | 1. Определение параметров.<br>2. Составление трехмерной матрицы отношений.<br>3. Преобразование матрицы отношений в двумерную таблицу.<br>4. Определение качественных и количественных значений показателей [8]. |
| | Многоуровневый подход. | Состояние системы защиты описывается совокупностью уровней конфиденциальности и набора категорий конфиденциальности. | Модель конечных состояний Белла Ла-Падулы. Решетчатая модель Д. Деннинга [9]. |
| | Оптимизационный (комбинаторный). | Решается задача дискретного программирования вида: максимизировать $\sum_{j=1}^{n}c_j x_j$ при условиях<br>$\sum_{j=1}^{n}a_{ij}x_j \le b_i, \quad i=\overline{1,m};$<br>$x_j \in \{0,1\}, \quad j=\overline{1,n}.$ | Методы Балаша для целочисленных переменных, ветвей и границ, исключения группы неизвестных, элементы теории двойственности, инструментарий линейного, выпуклого и параметрического программирования. |

Одним из способов оценки эффективности СЗИ является подход, обозначенный в таблице как оптимизационный или комбинаторный. При этом решается задача оптимизации вида: максимизировать некую функцию при заданных ограничениях.

Вид функции цели и система ограничений строятся в зависимости от нюансов поставленной задачи [10]. Так, если ввести нижеследующие обозначения, то можно рассмотреть несколько вариантов постановки.

Итак, пусть:

$U = \{u_j\}$ – множество угроз безопасности, j = 1,…m;

$A = \{a_i\}$ – множество механизмов безопасности, i = 1,…n;

$C = \{c_i\}$ – допустимые затраты на создание защиты (общий объем затрат), причем $c_i$ – это затраты на приобретение i-го средства защиты;

d(i,j) – эффективность нейтрализации i-м механизмом безопасности j-й угрозы.

Для построения математической модели введем переменные p(i,j) (y(ij)), равные 1, если j-я угроза устраняется с помощью i-го механизма, и нулю – в противном случае и q, такую, что

$$q(i,j)= \begin{cases} 1 - \textit{если } i - \textit{й механизм безопасности используется для устранения } j - \textit{й угрозы;} \\ 0 - \textit{в противном случае.} \end{cases}$$

Вначале считаем, что информационные угрозы между собой не связаны.

Первая задача – найти максимальный эффект от нейтрализации множества информационных угроз U с помощью задекларированных в системе средств защиты A при ограничениях на общий объем затрат C.

$$\sum_{j=1}^{m}\sum_{i=1}^{n} d(i,j)p(i,j) \Rightarrow \max \tag{1}$$

при ограничениях

$$\sum_{i=1}^{n} c(i) * sign \sum_{uj \in U}^{n} p(i,j) \le C \tag{2}$$

$$p(i,j) \in (1,0), \quad j = 1, \dots m; \quad i = 1,\dots n. \tag{3}$$

Вторая задача – вариант, когда уровень информационной безопасности определяется СЗИ с наименьшей эффективностью. В этом случае функция цели в формальной постановке задачи имеет вид:

$$\min \sum_{i=`1}^{n} d(i,j)p(i,j) \Rightarrow \max , \tag{4}$$

а ограничения (2) и (3) остаются теми же.

Третья задача – случай, когда появление одной угрозы $u_j$ является источником для другой, т.е. информационные угрозы не являются независимыми. В этом случае функция цели имеет вид (1), но пределы суммирования меняются – по первой сумме это перечень основных, а по второй – порожденных угроз. Вместо функции p(i,j) используется q(i,j).

Четвертая задача – это задача минимизации затрат на СЗИ при ограничении на заданный уровень эффективности. При этом алгоритм решения дополняется процедурой поиска максимальных элементов в каждом столбце матрицы d(i,j)

и расчетом наивысшего уровня эффективности Р, равным сумме найденных максимальных элементов:

$$\sum_{i=1}^{n} c_i * sign \sum_{j=1}^{m} p(i,j) \Rightarrow \min$$

$$\sum_{j=1}^{m}\sum_{i=1}^{n} d(i,j)p(i,j) / \sum_{i=1}^{n}(\max_j \ d(i,j) \le P;$$

$$p(i,j) \in (1,0), \ \ \text{j} = 1, \dots \text{m}; \ \ \text{i} = 1, \dots \text{n}.$$

Для решения задач указанного типа могут быть использованы методы Балаша для целочисленных переменных, ветвей и границ, исключения группы неизвестных, элементы теории двойственности, инструментарий линейного, выпуклого и параметрического программирования.

Повышение быстродействия рассматриваемых алгоритмов является актуальной задачей, т.к. между временем выполнения вычислений и размерностью задачи существует экспоненциальная зависимость. А размерность задачи, в свою очередь, зависит от сложности СЗИ, которая возрастает по мере появления новых угроз безопасности, и усложнением, связанным с развитием самой информационной системы, для которой создана система защиты.

Известно [11], что в аддитивном алгоритме Балаша требуется выполнение только операций сложения и вычитания, но процесс определения, существует ли дополнение решения, дающее значение целочисленной функции, превышающее текущую нижнюю оценку, поиск самой нижней оценки оптимального значения целочисленной функции не эффективен. Также при заданном частичном не всегда удается определить, какое значение должна иметь свободная переменная при любом допустимом дополнении и в случае, когда значение целевой функции превосходит текущую нижнюю оценку. В случае полного перебора, вычислительная сложность метода составляет $t(n) = O(n2^n)$ операций.

Метод ветвей и границ относится к комбинаторным методам. Со схемой вычислений по методу ветвей и границ можно ознакомиться в [11]. Вычислительная сложность метода $O(2^n(m+1))$, где $n$ – число вершин графа дерева решений, который образуется в процессе поиска решения, а m – количество ограничений.

К достоинствам метода следует отнести гибкость построения, позволяющую эффективно использовать специфику решаемой задачи. Однако исследователи отмечают зависимость объема вычислений, необходимых для решения задачи, от выбранной стратегии ветвления и способа вычисления оценок. Метод позволяет при построении верхних и нижних оценок функционала использовать эвристические методы и при определенных условиях получать точные или приближенные по функционалу с априорно заданной погрешностью решения.

Оба метода основываются на последовательном анализе вариантов, но используют различные подходы для отсева подмножеств, не содержащих оптимальных решений. В методе Балаша отсев производится на основании принципа оптимальности. В методе ветвей и границ отсев производится с применением нижних оценок на подмножествах.

Учитывая сказанное, сформулируем следующее утверждение: алгоритм, совмещающий положительные качества этих алгоритмов (операции целочисленного сложения и вычитания в алгоритме Балаша и продвижение по графу дерева решений в наилучшем направлении для метода ветвей и границ) является эффективным по сравнению с исходными с точки зрения теории вычислительной сложности.

Описание алгоритма.

Шаг 1. Задается значение функции цели так, чтобы оно соответствовало решению, при котором все p(i,j) = 0 (текущая нижняя оценка оптимального решения равна 0 ($z_0 = 0$). Возможно нахождение нижней оценки оптимального значения этой функции с помощью метода ветвей и границ.

Шаг 2. Проверить основной список задач и закончить вычисление, если он пуст. В противном случае выбрать очередную задачу из основного списка и вычеркнуть ее из него. При этом на множестве полученных оценок выделяют «лучшую» и ближайшую к ней.

Шаг 3. Установить, существует ли допустимое дополнение, у которого значение функции цели превосходит текущую нижнюю оценку оптимального решения. Если можно найти свободные переменные, которые должны иметь определенные значения при любом дополнении, когда значение целевой функции превосходит текущую нижнюю оценку оптимального решения, то следует расширить выбранное частичное решение. Если можно установить, что не существует допустимого дополнения, у которого значение целевой функции превосходит значение текущей нижней оценки оптимального решения, то положить $z_0^{(k+1)} = z_{[}^{(k)}$ и вернуться ко второму шагу. В противном случае перейти к четвертому шагу.

Шаг 4. Если расширенное частичное решение содержит все n переменных (т.е. является полным), то зафиксировать его и вернуться ко второму шагу. В противном случае перейти к пятому шагу.

Шаг 5. Выбирается любая свободная переменная, не входящая в расширенное частичное решение. Используются элементы метода ветвей и границ. Вводятся две новые задачи в основной список. В одной из них положить p(i,j) = 0 в расширенном решении, а в другой – p(i,j) = 1. Положить $z_0^{(k+1)} = z_0^{(k)}$ и вернуться ко второму шагу.

Шаг 6. Если зафиксировано допустимое решение, при котором целевая функция не изменилась, это решение оптимально.

Сокращение числа операций сравнений достигается благодаря выбору «лучшей» ближайшей оценки на втором шаге каждой итерации. Если считать, что ко второму шагу, содержащему элементы метода ветвей и границ, мы обращаемся в 3-х случаях из четырех, то вычислительная сложность комбинированного алгоритма составит $t'(n) = O(3n2^{n-2})$, что, естественно, меньше предыдущей оценки. Экспериментальная оценка подтверждает эффективность совмещенной стратегии движения по дереву решений.

Таким образом, предложен эффективный алгоритм решения задачи определения эффективности функционирования сложной системы.

Приведем методику оценки качества СЗИ с использованием оптимизационного подхода.

1. Составляется сценарий развития опасности (граф вида «дерево»), представляющий собой логико-вероятностную модель функционирования СЗИ. Это двудольный граф G (A,U), такой, что вершины множества в A отвечают аппаратным и программным средствам защиты, а вершины множеств в U – соответствующим информационным угрозам. Каждый элемент (вершина) множества A характеризуется ценой и эффективностью по нейтрализации информационных угроз. Каждой вершине множества U присваивается вес, равный стоимости, что соответствует СЗИ, а каждой дуге – вес p(i,j) = {1,0}. Конечное событие описывает опасное состояние системы.

2. Аналитически граф описывается с помощью целевой функции опасности системы и системы ограничений.

3. С помощью логико-вероятностных преобразований функция опасности системы приводится к одной из канонических форм и заменяется вероятностной функцией p(i,j). При этом необходимо иметь вероятности инициирующих событий, планируемые затраты на создание защиты и задать эффективность нейтрализации угрозы. Значение вероятностной функции p, при которой значение функции опасности и равно единице, определяет степень риска, присутствующего в системе.

4. Применяя только операции сложения и вычитания (алгоритм Балаша) находят частичные решения, при этом выбор на втором и пятом шагах может основываться на информации, полученной с помощью метода ветвей и границ.

Применяя эффективные правила выбора на втором и пятом шагах, можно найти допустимое по всем ограничениям и близкое к оптимальному решение уже на начальных итерациях.

Вычислительная сложность алгоритма тесно связана с числом целочисленных переменных. В данном алгоритме объем вычислений определяется прежде всего числом задач, входящих в основной список.

В заключение следует отметить графический способ демонстрации эффективности защиты, заключающийся в следующем (по аналогии с методом «ПАУК-ЦИС»).

Значение параметров элементов системы в начальный момент времени принимаем за 100 %. «Опасное» значение параметров соответствует воздействию максимального числа угроз на систему.

Диаграмма состояния строится в полярных координатах. Оси, на которых отмечаются значения параметров, направлены радиальные линии от центра окружности к периферии – это оси, на которых отмечаются значения параметров (рис. 1).

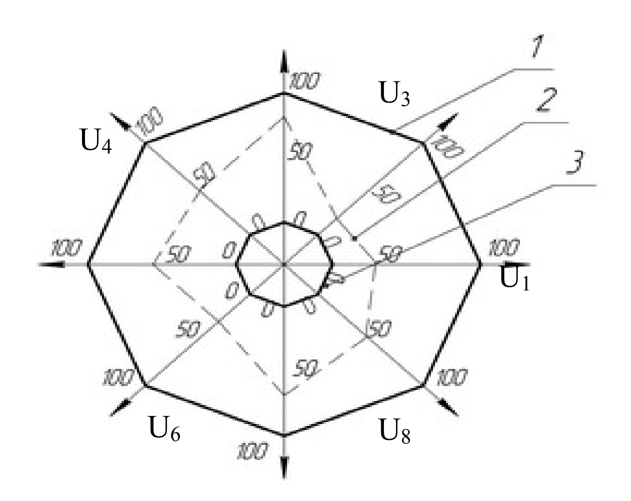



Рисунок 1 – Графический способ демонстрации эффективности системы защиты:
1 – нормальное состояние элемента системы; 2 – текущее состояние элемента системы; 3 – «опасное» состояние элемента информационной системы

Все данные откладываются на графике в процентах в начальный момент времени, каждый параметр равен 100 %. Строится фигура, которая будет отвечать допустимому состоянию системы. Эта фигура строится по минимальным величинам каждого из параметров. При пересечении фигурой 2 хотя бы в одной точке фигуры 3 следует срочно принимать меры по устранению угрозы безопасности.

При этом.

1. Количество контролируемых параметров для одного элемента технической системы должно быть не меньше двух.

2. Контролируемый параметр должен иметь количественную оценку.

3. Значения параметра откладываются на соответствующей оси в процентном выражении.

Возможна оценка состояния системы на основе анализа площадей многоугольников, а именно:

Начальное состояние элемента вычисляется по формуле (n – количество контролируемых системой параметров – угроз безопасности):

$$C_H = \frac{n}{2} \cdot R^2 \cdot \sin\alpha - S_c,$$

$S_c$ – площадь допустимого многоугольника:

$$S_c = \frac{n}{2} \cdot r^2 \cdot \sin\alpha,$$

$\alpha$ – центральный угол вычисляется по формуле: $\alpha = \frac{360}{n}$.

R – радиус описанной окружности, R=1.

Фактическое состояние системы: $C\phi = \sum_{i-1}^{n} S_i,$

Текущее изменение состояния системы влечет определение площади многоугольника, равной сумме площадей треугольников по формуле:

$$S_i = \frac{1}{2} \cdot (u_i \cdot u_{i+1}) \cdot \sin\alpha,$$

где $u_i$ – величина параметра.

Далее можно определить относительную или абсолютную величину защищенности системы:

$$D = C_H - (C_\Phi - S_c), \qquad Q = \frac{C\phi - S_c}{C_н}.$$

Параметр покажет, насколько элемент системы изменил свои свойства (в %) за определенный промежуток времени. После определения состояния каждого элемента системы выполняется оценка всей системы.

# Заключение

В одной статье невозможно описать все многообразие методов, применяемых для анализа эффективности СИБ. В числе других методов можно отметить методику оценки эффективности д.т.н. Г.Е. Шепитько, основанную на статистике угроз, критерий экономии от ущерба д.т.н. Э.И. Абалмазова и другие методы.

Полученные результаты свидетельствуют, что ни один из методов не лишен недостатков. Поэтому для решения подобных систем следует подобрать комбинацию методов, например, на первом этапе решать задачу комбинаторным методом по каждому из ограничений. Полученные в результате решения использовать для оценки верхней и нижней границы целевой функции. На втором этапе решать задачу методом

ветвей и границ и определить способ разбиения всего множества допустимых вариантов на подмножества, а также способ оценки верхней границы целевой функции. А с целью уменьшения числа вычислительных операций использовать метод Балаша.

# Литература

1. Киселев В.Д., Есиков О.В., Кислицын А.С. «Современные проблемы защиты в системах ее передачи и обработки» / Под ред. проф. Е.М. Сухарева. – М.:«Солид», 2000. – С. 200.
2. Шаньгин В.Ф., Соколов А.В. Защита информации в распределенных корпоративных сетях и системах. – Изд-во: ДМК, 2002. – 134 с.
3. Гарбарчук В., Зинович З., Свиц А. Кибернетический подход к проектированию систем защиты информации / Украинская академия информатики; Волынский гос. ун-т им. Леси Украинки; Люблинский политехнический ун-т. – К.; Луцк; Люблин, 2003. – 658 с.
4. Задірака В.К., Бабич М.Д., Березовський А.І. та ін. Т-ефективні алгоритми наближеного розв'язування задач обчислювальної математики. – К., 2003. – 216 с.
5. Маслова Н.А. Построение модели защиты информации с заданными характеристиками качества // Штучний інтелект. – Донецьк: ІШІ, 2007. – № 1. – С. 51-57.
6. Топольский Н.Г., Бутузов С.Ю. Основы создания проводящих сред для сверхскоростных информационных модулей автоматизированных систем безопасности. – М.: Ак. ГПС МВД России, 2001.
7. Чипига А.Ф., Пелешенко В.С. Оценка эффективности защищенности автоматизированных систем от несанкционированного доступа.
8. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – Изд-во «ДиаСофт», 2002. – 693с.
9. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – М: Наука и техника, 2003. – 384 с.
10. Росс Г.В. Моделирование производственных и социально-экономических систем с использованием аппарата комбинаторной математики. – М.: Мир, 2001. – 176 с.
11. Зайченко Ю.П. Исследование операций: Учебник. – 6-е изд., перераб. и доп. – К.: Изд. дом «Слово», 2003. – 688 с.

***Н.О. Маслова***
**Методи оцінки ефективності систем захисту інформаційних систем**
У роботі класифікований підхід до визначення якості систем захисту інформації, наведені показники оцінки якості й особливості розрахунку показників. Описана модифікація алгоритму Балаша, яка дозволяє мінімізувати обчислювальні витрати за рахунок використання цілочисельних перемінних, операцій додавання і вирахування і вибору кращого напрямку спуску деревом рішень, властивого методам типу гілок і границь. Запропоновано методику обчислювальної складності алгоритму, який використовує цю модифікацію.

*Статья поступила в редакцию 15.07.2008.*